470TH MI BDE ACCEPTABLE USE POLICY FOR INFORMATION SYSTEMS (IS)

REFERENCES:

a. Army Regulation (AR) 25-2, Information Assurance, 24 October 2007

b. ALARACT 157/2008 DTG JUN 08

c. Information Assurance Best Business Practice for Army Password Standards, 1 May 2008

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in 470th MI BDE networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. No access to IS is authorized until the user completes the training specified in this policy. **Only appointed Information Transfer Agents (ITA) are authorized to transfer information from classified IS.**

2. Access. Access to this/these network(s) is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring, and security testing.

4. Classified information processing. The SIPRNET LAN is the primary classified Information Systems (IS) for 470th MI BDE. The SIPRNET LAN is a US-only system and approved to process SECRET collateral information as well as: NOFORN, ORCON. The SIPRNET LAN is not authorized to process TOP SECRET or SCI.

a. The SIPRNET LAN provides communication to external DoD organizations using the SIPRNET. Primarily this is done via electronic mail and internet networking protocols.

b. The SIPRNET LAN is authorized for SECRET or lower-level processing in accordance with the Site's SIPRNET accreditation.

c. The classification boundary between SIPRNET, JWICS, NSANET and NIPRNET LANs require vigilance and attention by all users. The SIPRNET LAN is also a US-only system and not accredited for transmission of NATO material.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET or SCI information through the SIPRNET LAN is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. Unclassified information processing. The NIPRNET LAN is the primary unclassified automated administration tool for the 470th MI BDE. The NIPRNET LAN is a US-only system.

a. The NIPRNET LAN provides unclassified communication to external DoD and other US Government organizations. Primarily this is done via electronic mail and the Internet networking protocols such as web, ftp, and telnet.

b. The NIPRNET LAN is approved to process UNCLASSIFIED, SENSITIVE information in accordance with the Site's NIPRNET accreditation.

c. The NIPRNET LAN and the Internet, as viewed by the 470th MI BDE, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of Confidential, SECRET, TOP SECRET or SCI information through the NIPRNET LAN is a security violation and will be investigated and handled as a security violation or as a criminal offense.

Initials_____

6. Minimum security rules and requirements. As a 470th MI BDE system user, the following minimum security rules and requirements apply to all 470th MI BDE networks :

a. Personnel are not permitted access to the SIPRNET LAN and the NIPRNET LAN unless in complete compliance with the 470th MI BDE personnel security requirement for operating in a SECRET system-high environment.

b. I have completed the online, "DoD Information Assurance Awareness Training", "Marking Classified Information", and "Wide Network Security Focus" courses. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I know I will be issued a unique identifier and a password to authenticate my identifier (that is, a user ID). After receiving my user ID:

- I will protect the password that authenticates the identifier.
- If I am assigned an individual user account, I will not permit anyone else to use my password, nor will I reveal my password to anyone else. If my account is on a classified network, I will protect the password in accordance with the level of the network's classification level.
- I am responsible for all activity that occurs on my individual account once my password has been used to log on.
- I will change my password every 60 days.
- I will not store my password on any processor or microcomputer or on any magnetic or electronic media unless approved in writing by the Information Assurance Manager (IAM)/Information Assurance Security Officer (IASO).
- I will not tamper with my computer to avoid adhering to the password policy.
- I will never leave my computer unattended while I am logged on unless protected by a "password-protected" screensaver.

d. I will generate, store, and protect passwords or pass-phrases. IAW AR 25-2, passwords will consist of at least 15 characters with 2 each of following: Uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not allow any individual to have access to my account nor use my login information. (I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)

e. I will use only the authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

f. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

g. I will not attempt to access or process data exceeding the authorized IS classification level.

h. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

i. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

j. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

k. I will not utilize Army- or DoD-provided ISs for commercial financial gain or illegal activities.

l. Maintenance will be performed by the System Administrator (SA) only.

m. I will use screen locks and log off the workstation when departing the area.

n. I will immediately report any suspicious output, files, shortcuts, or system problems to the 470th MI BDE SA and/or IASO and cease all activities on the system.

o. I will address any questions regarding policy, responsibilities, and duties to the 470th MI BDE SA and/or IASO.

p. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

q. I understand that monitoring of the NIPRNET, SIPRNET, NSANET and BL-COL (Centrix) LANs will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities are prohibited and define unacceptable uses of an Army IS:

- Pornography or obscene material (adult or child)
- Copyright infringement (including the sharing of copyright material by means of peer-to-peer software)
- Gambling
- Transmission of chain letters
- Unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use
- Violation of any statute or regulation
- Hateful, harassing, or other antisocial behavior
- Release of information about the Government that has not been approved for disclosure
- Disclosure of restricted information to unauthorized recipients
- Sending sensitive or classified information in clear text (unencrypted) over the Internet
- Hacking or attempting to hack into IS
- Playing or installing unauthorized games including web based
- Other inappropriate activities

9. Keyboard, Video, Monitor (KVM) Switches. This process must be performed for each switch between system. When the system is not in use, it is required to be inactive and displaying the screen lock. Any suspected tampering and/or mishandling of a KVM will be reported to the SSO or IAM immediately.

a. Logging onto a system.

- Identify the classification of the system currently selected
- Use the login and passwords appropriate to that system
- Verify the classification of the present system by checking the classification label
- Begin processing

b. Switching between systems.

- Screen lock the system you are currently working on
- Select desired system with the KVM switch
- Enter your user id and password to deactivate the screen lock
- Verify the classification of the present system by checking the classification label

c. Logging off of a system.

- Close all applications processing on the active system

- Logout of the system when processing is no longer required on the system
- Logout of system at the end of duty day

10. Thumb Drives. Thumb Drives are not authorized for use on Army networks

11. Standard Mandatory DoD Notice & Consent Banner.
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

- For Blackberries and other PDAs/PEDs with severe character limitations:

  - I've read & consent to terms in IS user agreement.

12. Standard Mandatory Notice and Consent Provision for all DoD Information System User Agreements.
By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

a. You are accessing a U.S. Government (USG) IS (which includes any device attached to this IS) that is provided for USG authorized use only.

b. You consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes of including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using an IS does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any USG actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an IS, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data in not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection or a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an IS if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take responsible steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waiver the privilege or confidentiality of such protections otherwise exist under established legal standards and DoD policy. However, in such cases the USG is authorized to take reasonable actions to identify such communications or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the USG shall take reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the USG may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the USG's otherwise-authorized use or disclosure of such information.

- All of the above conditions apply regardless or whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

12. Acknowledgement. I have read the above requirements regarding use of 470th MI BDE information systems and agree to its terms. I understand my responsibilities regarding these systems and the information contained in them.

_____	_____
Command/ Section	Phone Number
_____	_____
Last Name, First, MI	Rank/Grade
_____	_____
Signature	Date